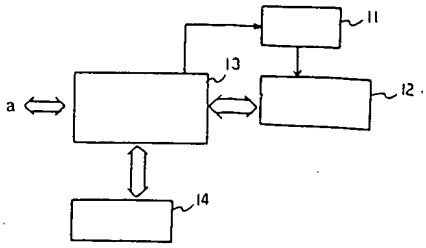
(54) **INFORMATION PROCESSOR**
(11) **2-205913 (A)** (43) 15.8.1990 (19) JP
(21) Appl. No. 64-25073 (22) 3.2.1989
(71) SEIKO EPSON CORP (72) KATSUMI TSUKADA
(51) **Int. Cl⁵. G06F3/06,G11B19/02**

PURPOSE: To reduce the frequency in access to a fixed disk to reduce the power consumption of the fixed disk by providing a means which accesses a semiconductor memory at the time of issue of a request command for information from a central processing unit and turning on the power source of a fixed disk device to operate it at the time of absence of required information in this memory.

CONSTITUTION: When an information request from a host is issued to a fixed disk device controller 13, a semiconductor memory 14 is first accessed, and required information is taken from the semiconductor memory when existing in this memory 14. When required information does not exist in the memory 14, a power source 11 of a fixed disk device 12 is started to take information from the fixed disk device 12. Information is directly written in the fixed disk device 12. Thus, power supply to the fixed disk device and rotation of a disk are stopped when the fixed disk device is not accessed, and the power consumption of the fixed disk device is reduced.

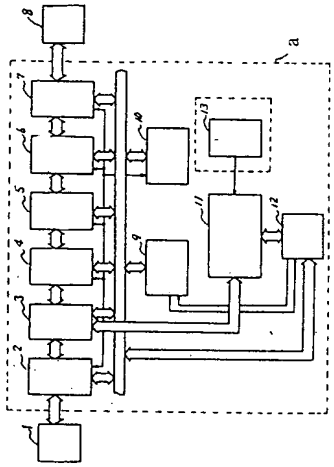


a: host

(54) **OPTICAL DISK PROCESSOR**
(11) **2-205914 (A)** (43) 15.8.1990 (19) JP
(21) Appl. No. 64-25406 (22) 3.2.1989
(71) GUNMA NIPPON DENKI K.K. (72) SEIICHI YAMAGUCHI
(51) **Int. Cl⁵. G06F3/06,G06F3/08,G11B20/10**

PURPOSE: To perform the high speed processing by recording and reproducing information in and from a disk-shaped storage medium with a first microprocessor and recording and reproducing information in and from a storage means independent of the storage medium with a second microprocessor.

CONSTITUTION: When the read operation will be executed with a first microprocessor 9, a second microprocessor 12 checks whether pertinent data exists in a semiconductor memory or not; and when this data exists there, the second microprocessor 12 interrupts the first microprocessor 9 to transfer data on the semiconductor memory to a host system in place of the first microprocessor 9. When the second microprocessor 12 cannot find pertinent data in the semiconductor memory, data read out by the first microprocessor 9 is recorded on the semiconductor memory through a bus selector circuit 3 by the second microprocessor 12 itself. Thus, the microprocessor which fast finds pertinent data transfers data, and the high speed processing is possible.

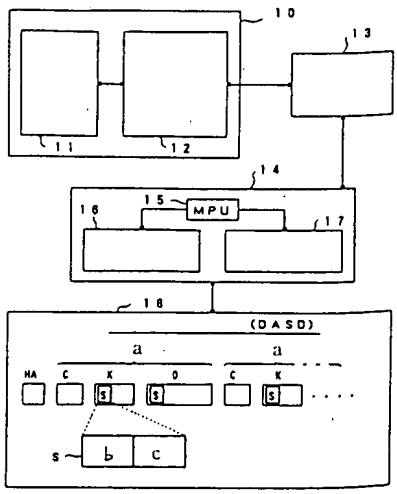


1: host system, 2: host interface control, 4: bus buffer, 5: error correcting circuit, 6: modulating/demodulating circuit, 7: drive interface, 8: optical disk drive, 10: sector control, 11: semiconductor memory, 13: battery backup, a: controller

(54) **RECORD UNIT SECURITY CONTROL SYSTEM**
(11) **2-205915 (A)** (43) 15.8.1990 (19) JP
(21) Appl. No. 64-25219 (22) 3.2.1989
(71) FUJITSU LTD (72) KATSUTOSHI MURAMATSU
(51) **Int. Cl⁵. G06F3/06,G06F12/14**

PURPOSE: To realize a high-density security system with a security protection range as the record unit by adding security information to a record.

CONSTITUTION: Security information is added to each record itself stored in a direct access storage device 18, and it is checked whether each record can be accessed or not by a controller 14 at the time of reading and writing the record. Consequently, the execution of an input/output request which ignores security information is suppressed by the controller 14 to protect the security of each record in the direct access storage device 18. An input/output management part 12 adds a channel program, which sets security information, before a user's channel program (CCW) to designate security information which is used to discriminate whether the access is possible or not. Thus, security protection is performed with a record as the unit without changing the current user's channel program.



10: processor (CPU/memory), 11: access request part, 13: channel device, 16: security information recording control part, 17: security information checking part, S: security label, a: record, b: level (L), c: category (C)

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−205915

⑤Int.Cl.⁵	識別記号	庁内整理番号
G 06 F 3/06	304 H	6711−5B
12/14	320 A	7737−5B

⑬公開　平成2年(1990)8月15日

審査請求　未請求　請求項の数 1　(全8頁)

⑤④発明の名称　レコード単位セキュリテイ制御方式

⑳特　願　平1−25219
㉒出　願　平1(1989)2月3日

⑦②発明者　村松　勝利　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
⑦①出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
⑦④代理人　弁理士　小笠原　吉義　外2名

明　細　書

1．発明の名称

レコード単位セキュリティ制御方式

2．特許請求の範囲

カウント部，キー部，データ部を有する記録フォーマットによって，レコード情報の記憶が行われる直接アクセス記憶装置(18)におけるレコードの機密保護を行うレコード単位セキュリティ制御方式であって，

上記直接アクセス記憶装置をコントロールする制御装置(14)内に，

レコード単位にアクセス可否の決定に使用されるセキュリティ情報を付加して直接アクセス記憶装置内に記録する制御手段(16)と，

レコードの読み出しおよび書き込み時に，指定されたセキュリティ情報と，アクセス対象となるレコードに付加されたセキュリティ情報との照合により，アクセス可否を決定するセキュリティ情報検査手段(17)とを備えたことを特徴とするレコード単位セキュリティ制御方式。

3．発明の詳細な説明

(概要)

カウント部，キー部，データ部を有する記録フォーマットによって，レコード情報の記憶が行われる直接アクセス記憶装置におけるレコードの機密保護を行うレコード単位セキュリティ制御方式に関し，

レコード単位の高密度のセキュリティシステムを実現可能とすることを目的とし，

直接アクセス記憶装置をコントロールする制御装置内に，レコード単位にアクセス可否の決定に使用されるセキュリティ情報を付加して直接アクセス記憶装置内に記録する制御手段と，レコードの読み出しおよび書き込み時に，指定されたセキュリティ情報と，アクセス対象となるレコードに付加されたセキュリティ情報との照合により，アクセス可否を決定するセキュリティ情報検査手段

とを備えるように構成する。

〔産業上の利用分野〕

本発明は，カウント部，キー部，データ部を有する記録フォーマットによって，レコード情報の記憶が行われる直接アクセス記憶装置におけるレコードの機密保護を行うレコード単位セキュリティ制御方式に関する。

計算機システムの高度な利用により，真に権限を持つ者だけがデータを読み書きできるようなデータの機密保護の技術がますます重要になってきている。応用分野によっては，機密保護の単位を，ファイルのようなデータの大きな集合だけではなく，レコード単位とすることが必要になる場合がある。

〔従来の技術〕

計算機システムが扱うデータに対して，不当なアクセスを防ぐために，アクセス制御，フロー制御，暗号化など，種々のセキュリティ方式が考えられている。

データのセキュリティは，データを使用する正当な権限のある処理主体にのみ，そのデータの使用を許可することにより実現される。データが，磁気ディスク装置などの直接アクセス記憶装置（ＤＡＳＤ）に記録されたものである場合には，その直接アクセス記憶装置に対するＩ／Ｏを発行し，それに記憶されたデータを参照したり，変更したりすることが，正しい権限のもとで行われる必要がある。

このような機密保護の単位としては，ボリュームやファイルなどがあり，従来，主としてオペレーティング・システム（ＯＳ）の制御によって実現されている。しかしながら，直接アクセス記憶装置に記録されている各レコード単位に，セキュリティ機能を設定する手段は実現されていなかった。

〔発明が解決しようとする課題〕

１つのファイルが，多数の可変長レコードから構成される場合に，個々のレコードの種類ごとに，そのデータに対する参照または更新を許可したり，禁止したりすることができるようにすることが必要になる場合がある。

しかし，従来方式では，レコード単位にセキュリティ機能を設定することができないため，機密保護レベルに応じてファイルを分割し，それぞれ機密保護レベルが同等なレコード群をまとめて，別々なファイルとして作成する必要があった。

この場合，一連のデータ処理において，多数のファイルをアクセスしなければならないようなことが起こり，処理が複雑化するとともに，処理時間やメモリが多く必要になるという問題があった。

また，ソフトウェアによる論理操作によって，主記憶装置に展開されたレコード内のデータの使用可否を決定することも考えられているが，本体系処理装置のソフトウェアによる対処だけでは，直接アクセス記憶装置におけるレコードの不当なアクセスを，直接禁止することができないので，機密保護が十分ではないという問題があった。

また，セキュリティ情報を，その機密保護対象となるレコードとは別の場所で記憶し管理する場合には，セキュリティ情報自体の改ざん防止のために，さらにその機密保護手段が必要になるという問題があった。

本発明は上記問題点の解決を図り，レコード単位の高密度のセキュリティシステムを実現可能とすることを目的としている。

〔課題を解決するための手段〕

第１図は本発明の原理ブロック図を示す。

第１図において，１０はＣＰＵおよびメモリなどからなる処理装置，１１は各レコードに対するアクセス要求を行うアクセス要求部，１２はオペレーティング・システムにおける入出力動作を管理する入出力管理部，１３はチャネル装置，１４は配下に接続される装置をコントロールする制御装置，１５はマイクロプロセッサ（ＭＰＵ），１６はセキュリティ情報記録制御部，１７はセキュリティ情報検査部，１８はディスクパック装置な

どの直接アクセス記憶装置を表す。

直接アクセス記憶装置１８は，本発明において機密保護の対象とするレコードを記憶する装置であって，カウント部Ｃ，キー部Ｋ，データ部Ｄを有する記録フォーマットにより，レコード情報を記憶するようになっている。なお，ＨＡはトラックの先頭を示すホームアドレスである。

本発明では，各レコードにセキュリティラベルＳが付加されるようになっている。セキュリティラベルＳは，機密度の程度を示すレベル（Ｌ）と，適用範囲を示すカテゴリ（Ｃ）とからなる。この例では，セキュリティラベルＳは，キー部Ｋとデータ部Ｄとに，同内容のものが格納されるようになっている。キー部Ｋとデータ部Ｄとに，セキュリティラベルＳを持つのは，レコードへの位置付けやデータの読み書きにおけるセキュリティの検査を，位置付け時または位置付け後にそれぞれ独立に行うことができるようにし，処理を高速化するためである。

このセキュリティラベルＳにより，レコード単位のセキュリティを実現するために，制御装置１４は，ファームウェアによるセキュリティ情報記録制御部１６と，セキュリティ情報検査部１７とを持つ。

セキュリティ情報記録制御部１６は，レコードのカウント部Ｃ，キー部Ｋ，データ部Ｄを，直接アクセス記憶装置１８に書き込むときに，セキュリティラベルＳを付与して記録する制御を行う。

セキュリティ情報検査部１７は，レコードの読み出しおよび書き込み時に，先行するチャネルコマンドによって指定されたセキュリティ情報と，レコードに付加されたセキュリティラベルＳとの照合により，そのレコードに対するアクセス可否を決定する制御を行うようになっている。

〔作用〕

本発明では，直接アクセス記憶装置１８に格納されたレコード自体に，セキュリティ情報が付加され，レコードの読み出しおよび書き込み時には，制御装置１４によって，各レコードに対するアクセス可否のチェックが行われる。したがって，セキュリティ情報を無視した入出力要求は，制御装置１４により，その実行が抑止され，直接アクセス記憶装置１８における各レコードの機密保護が達成される。

アクセス可否の決定に使用するセキュリティ情報の指定は，ユーザのチャネルプログラム（ＣＣＷ）の前に，入出力管理部１２が，セキュリティ情報を設定するチャネルプログラムを付加するようにすれば，現状のユーザのチャネルプログラムを変更することなく，レコード単位の機密保護を図ることができる。

セキュリティの検査は，制御装置１４によって自動的に行われるので，処理装置１０におけるソフトウェアのオーバヘッドはほとんどない。

〔実施例〕

第２図は本発明の実施例によるレコード形式の例，第３図は本発明の実施例に係るディスク制御装置構成図，第４図は本発明の実施例によるデータ読み込みコマンドの例，第５図は本発明の実施例によるデータ読み込み制御の例，第６図は本発明の実施例によるデータ読み込み時のセキュリティ・チェックの例，第７図は本発明の実施例によるデータ書き込みコマンドの例，第８図は本発明の実施例によるデータ書き込み制御の例，第９図は本発明の実施例によるデータ書き込み時のセキュリティ・チェックの例を示す。

本発明は，可変長レコードを記録する直接アクセス記憶装置，いわゆるＣＫＤ－ＤＡＳＤにおけるレコード情報の機密保護を扱う。そのレコード形式は，第２図に示すようになっている。セキュリティラベルＳに関する情報が付加されること以外は，従来と同様な構成である。

カウント部Ｃは，次の情報を持つ。

・Ｐ：フラグ（このフラグとして，従来形式であるか，セキュリティラベルＳを持つ拡張形式であるかの表示が追加される）。
・ＣＣ：シリンダ番号。
・ＨＨ：ヘッド番号。

・Ｒ：レコード番号。
・Ｓ：セキュリティラベルの長さ（新設）。
・Ｋ：キー部の長さ。
・ＤＤ：データ部の長さ。

また，キー部Ｋとデータ部Ｄの先頭に，それぞれセキュリティラベルＳが記録される。キー部ＫにおけるセキュリティラベルＳの内容と，データ部Ｄにおけるセキュリティラベルの内容とは同じである。

第３図（イ）は，本発明の実施例であるディスク制御装置２０の構成例を示している。

ディスク制御装置２０は，上位のチャネル装置と，直接アクセス記憶装置であるディスクパック装置２４との間に接続され，ディスクパック装置２４をコントロールする。チャネル装置側にチャネル・インタフェース２１を有し，ディスクパック装置２４側にデバイス・インタフェース２３を有する。また，これらのインタフェースをマイクロプログラムによって制御するマイクロプロセッサ１５と，データバッファ２２とを持つ。

データバッファ２２には，第３図（ロ）に示すように，セキュリティ情報セーブ域２５，チャネルコマンドが格納されるコマンドバッファ２６，セキュリティ情報の判定結果を記憶するセキュリティ情報判定結果記憶部２７および入出力レコードに関するカウントバッファ２８，キーバッファ２９，データバッファ３０が設けられる。

第４図は，セキュリティラベルＳが付加されたレコードのデータを読み込む場合に使用するチャネルコマンドの例を示している。ここでは，以下のような(a)～(e)のコマンドによってチャネルプログラムが作成されている。

(a)　ＳＳＤ：セキュリティ情報設定コマンド

新しくセキュリティ情報を指定するために設けられたコマンドである。このＳＳＤコマンドでは，セキュリティラベルＳに対応するレベルとカテゴリとを指定する。レベルおよびカテゴリの長さは，それぞれ用途に応じて変化し，可変長である。

(b)　ＴＩＣ：分岐コマンド

ここから，ユーザが作成したチャネルプログラム（ＣＣＷ）に分岐する。すなわち，この(a)，(b)のコマンドは，第１図に示す入出力管理部１２が，アクセス要求部１１が作成したチャネルプログラムに付加するようにしたコマンドである。

(c)　ＳＩＤ：サーチＩＤコマンド
(d)　ＴＩＣ：分岐コマンド
(e)　ＲＤ：リードデータコマンド

この(c)～(e)のコマンドは，ＣＫＤ－ＤＡＳＤに対するアクセスに，従来から使用されているコマンドである。

第４図に示すようなチャネルコマンドに対し，第３図に示すディスク制御装置２０のマイクロプロセッサ１５は，第５図に示すような制御を行う。

(a)　ＳＳＤコマンドに対して，データバッファ２２におけるセキュリティ情報セーブ域２５に，コマンドで指定されたセキュリティ情報を退避する。
(b)　次にＴＩＣコマンドに対して，データ読み込みを行う以下のユーザＣＣＷへ分岐する。
(c)　ＳＩＤコマンドに対して，直接アクセス記憶装置から，レコードのカウント部をデータバッファ２２へ読み込み，指定されたレコードのカウント部かどうかを検査する。指定された位置ではない場合，サーチが終了するまで，カウント部の検査を繰り返す。

指定された位置のカウント部である場合，次にキー部またはデータ部のセキュリティラベルＳと，セキュリティ情報セーブ域２５に退避したセキュリティ情報とを比較照合し，位置付けの可否を決定する。

(d)　位置付けが「可」である場合，ＴＩＣコマンドの次に移る。「不可」であれば，(c)のサーチを繰り返す。
(e)　ＲＤコマンドに対し，データ部のセキュリティ情報を比較して，アクセス可であれば，データ部のデータを読み込む。アクセス不可の場合，Ｉ／Ｏエラーとする。ここでのセキュリティ情報のチェックは，このＲＤコマンドが，ＳＩＤ＋ＴＩＣのコマンドにチェインされていた場合には，省略することができる。ＲＥＡＤ系またはＷＲＩＴＥ系のコマンドにチェインされていた場合には，

必ずチェックを行う。

例えば，データの読み込み時に，第6図（イ）に示すセキュリティ情報を，ＳＳＤコマンドで指定したとする。レベル情報Ｌは，値が大きいほうが機密度が高い。カテゴリ情報Ｃは，ここでは情報の種類ごとに，１ビットのフラグで定義している。今，ＳＳＤコマンドで指定したレベルおよびカテゴリを，ＳＳＤ－Ｌ，ＳＳＤ－Ｃとし，レコード内に設定されているセキュリティラベルＳのレベルおよびカテゴリを，レコード－Ｌ，レコード－Ｃとすると，データ読み込みが可能である条件は，以下のとおりである。

ＳＳＤ－Ｌ≧レコード－Ｌ　かつ

ＳＳＤ－Ｃ⊃レコード－Ｃ

第6図（イ）に示すセキュリティ情報の指定により，第6図（ロ）に示すようなレコードに対するデータの読み込みが行われた場合，上記セキュリティ条件により，１番目と２番目のレコードは，読み込み可となる。３番目のレコードに対して，読み込みが指示されたとすると，レベルが合わないため，Ｉ／Ｏエラーとなる。

第6図（ハ），（ニ）は，他の例を示している。

第6図（ハ）に示すセキュリティ情報の指定により，第6図（ニ）に示すようなレコードに対するデータの読み込みが行われた場合，１番目のレコードは，カテゴリが満足しないので，読み込み不可である。３番目のレコードは，レベルが合わないので，読み込み不可である。したがって，２２番目だけが読み込み可能なレコードとなる。

第7図は，セキュリティラベルＳが付加されたレコードに，データを書き込む場合に使用するチャネルコマンドの例を示している。(a)～(d)のコマンドは，第4図に示したデータ読み込み時におけるコマンドと同様であり，(e)のＷＤコマンドは，データを書き込むことを指示するコマンドである。

この第7図に示すチャネルコマンドに対し，第3図に示すディスク制御装置２０のマイクロプロセッサ１５は，第8図に示すような制御を行う。

(a)　ＳＳＤコマンドに対して，データバッファ２２におけるセキュリティ情報セーブ域２５に，コマンドで指定されたセキュリティ情報を退避する。

(b)　次にＴＩＣコマンドに対して，データ読み込みを行う以下のユーザＣＣＷへ分岐する。

(c)　ＳＩＤコマンドに対して，直接アクセス記憶装置から，レコードのカウント部をデータバッファ２２へ読み込み，指定されたレコードのカウント部かどうかを検査する。指定された位置ではない場合，サーチが終了するまで，カウント部の検査を繰り返す。

指定された位置のカウント部である場合，次にキー部またはデータ部のセキュリティラベルＳと，セキュリティ情報セーブ域２５に退避したセキュリティ情報とを比較照合し，位置付けの可否を決定する。

(d)　位置付けが「可」である場合，ＴＩＣコマンドの次に移る。「不可」であれば，(c)のサーチを繰り返す。

(e)　ＷＤコマンドに対し，データ部のセキュリティ情報を比較して，アクセス可であれば，データ部のデータを書き込む。アクセス不可の場合，Ｉ／Ｏエラーとする。ここでのセキュリティ情報のチェックは，このＷＤコマンドが，ＳＩＤ＋ＴＩＣのコマンドにチェインされていた場合には，省略することができる。ＲＥＡＤ系またはＷＲＩＴＥ系のコマンドにチェインされていた場合には，必ずチェックを行う。

例えば，データの書き込み時に，第9図（イ）に示すセキュリティ情報を，ＳＳＤコマンドで指定したとする。ＳＳＤコマンドで指定したレベルおよびカテゴリを，ＳＳＤ－Ｌ，ＳＳＤ－Ｃとし，レコード内に設定されているセキュリティラベルＳのレベルおよびカテゴリを，レコード－Ｌ，レコード－Ｃとすると，データ書き込みが可能である条件は，以下のとおりである（ＲＥＡＤ時の条件とは逆の関係になる）。

ＳＳＤ－Ｌ≦レコード－Ｌ　かつ

ＳＳＤ－Ｃ⊂レコード－Ｃ

第9図（イ）に示すセキュリティ情報の指定により，第9図（ロ）に示すようなレコードに対するデータの書き込みが行われた場合，上記セキュ

リティ条件により，2番目と3番目のレコードは，書き込み可となる。1番目のレコードに対して，書き込みが指示されたとすると，レベルが合わないため，I／Oエラーとなる。

第9図（ハ），（ニ）は，他の例を示している。

第9図（ハ）に示すセキュリティ情報の指定により，第9図（ニ）に示すようなレコードに対するデータの書き込みが行われた場合，結果として書き込み可能なレコードは，3番目のレコードだけとなる。

なお，セキュリティ情報の扱いについて，SSDコマンド以外に，必要に応じて種々のコマンドをサポートすることは，制御装置におけるファームウェアの変更により，容易に対処することができる。例えば，互換性のため，カウント部，キー部，データ部を合わせて読み込むコマンド（READ CKDコマンド）では，セキュリティラベルSの情報を取り除いて通知する。セキュリティラベルSを読むために，次のようなコマンド，

① READ C&Sコマンド
② READ K&Sコマンド
③ READ KD&Sコマンド
④ READ CKD&Sコマンド

などを新設する。WRITE系のコマンドに対しても，同様にセキュリティラベルSを設定するフォーマット用のコマンドを用意する。

〔発明の効果〕

以上説明したように，本発明によれば，レコードにセキュリティ情報を付加することにより，権限を持つ処理主体だけが，読み書きできるようになるので，セキュリティ保護範囲をレコード単位として，高密度のセキュリティシステムを実現することができるようになる。また，セキュリティ情報をレコードに持つので，データの移動に対しても保護が外れることがなくなり，コピーなどの不正使用についても防止することができる。

4．図面の簡単な説明

第1図は本発明の原理ブロック図，

第2図は本発明の実施例によるレコード形式の例，

第3図は本発明の実施例に係るディスク制御装置構成図，

第4図は本発明の実施例によるデータ読み込みコマンドの例，

第5図は本発明の実施例によるデータ読み込み制御の例，

第6図は本発明の実施例によるデータ読み込み時のセキュリティ・チェックの例，

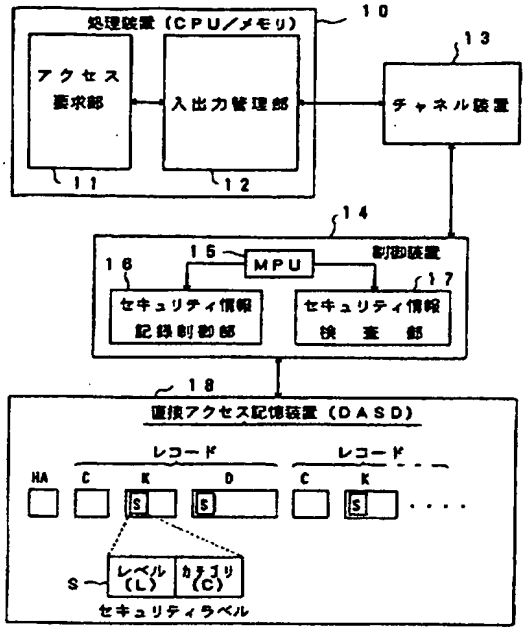
第7図は本発明の実施例によるデータ書き込みコマンドの例，

第8図は本発明の実施例によるデータ書き込み制御の例，

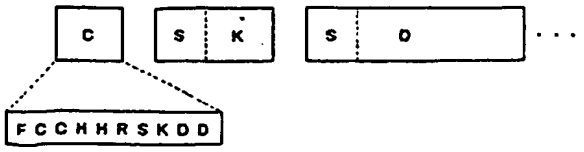
第9図は本発明の実施例によるデータ書き込み時のセキュリティ・チェックの例を示す。

図中，10は処理装置，11はアクセス要求部，12は入出力管理部，13はチャネル装置，14は制御装置，15はマイクロプロセッサ，16はセキュリティ情報記録制御部，17はセキュリティ情報検査部，18は直接アクセス記憶装置，Sはセキュリティラベルを表す。

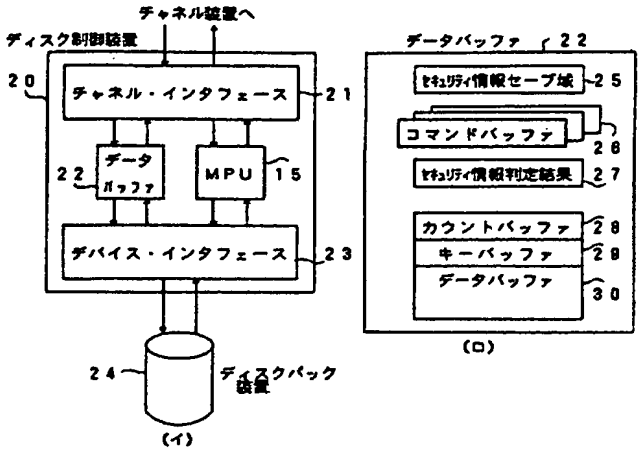
特許出願人　富士通株式会社
代理人　弁理士　小笠原吉義（外2名）



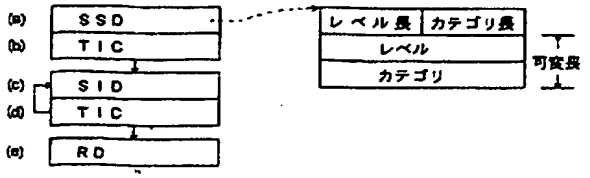
本発明の原理ブロック図
第 1 図



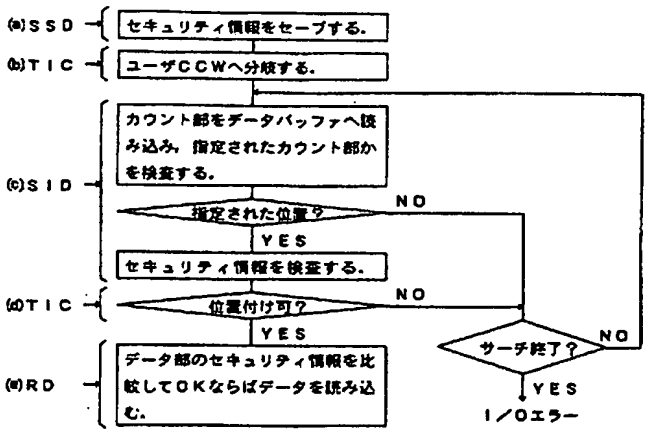
レコード形式の例
第 2 図



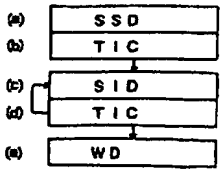
ディスク制御装置構成図
第 3 図



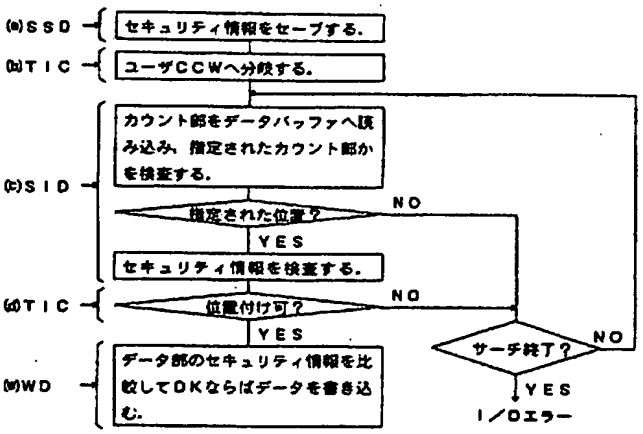
データ読み込みコマンドの例
第 4 図



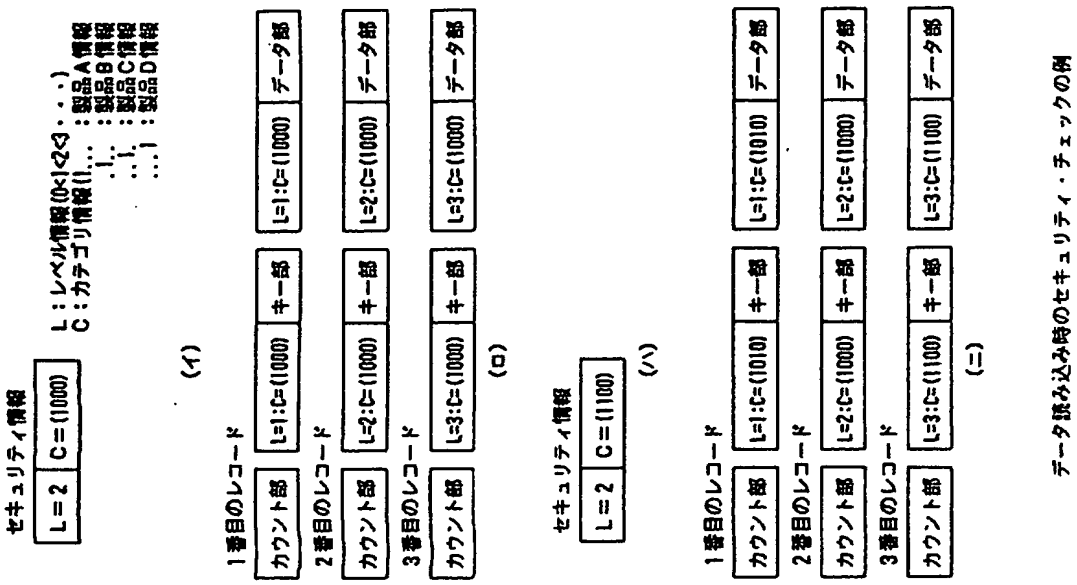
データ読み込み制御の例
第 5 図



データ書き込みコマンドの例
第 7 図

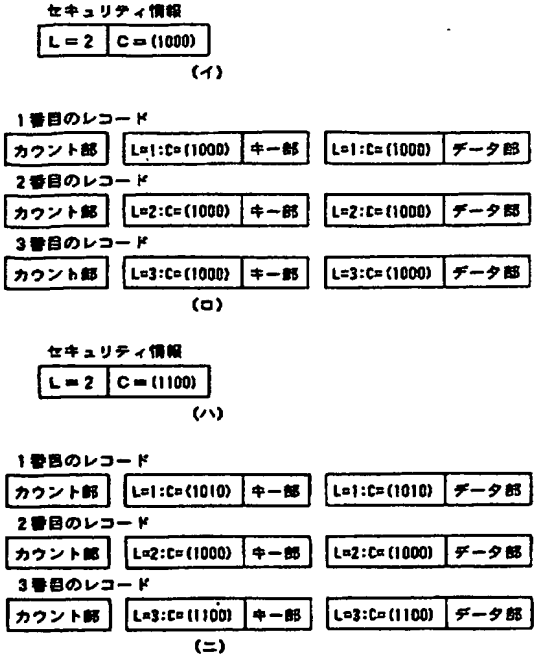


データ書き込み制御の例
第 8 図



データ読み込み時のセキュリティ・チェックの例

第 6 図



データ書き込み時のセキュリティ・チェックの例

第 9 図